IN THE CLAIMS

Please amend claims 1-12 as follows:

1. (Currently Amended) A tamper-resistant fault detection ~~processing~~ method for an IC card including ~~performing a symmetric-key encryption process utilizing~~ an information processing device mounted thereon, comprising the steps of:

(1) performing a[[n]] symmetric-key encryption process Z = E (M, K) in which a secret key K is to be applied to an input plaintext M, and [[for]] storing a processing result Z in a memory in the IC card;

(2) performing a corresponding decryption process W = D (Z, K) for said process result Z stored on said memory and storing the decryption result W on the memory;

(3) outputting said processing result Z from said information processing device when said processing result W coincides with said plaintext M; and

(4) suppressing the output of said processing result Z from said information processing device when said processing result W does not coincide with said plaintext M.

2. (Currently Amended) [[An]] The encryption processing method of claim 1 wherein said encryption process and said decryption process are executed according to the DES (data encryption standard).

3. (Currently Amended) [[An]] The encryption processing method of claim 1 wherein said information processing device is reset as a control method of suppressing the output of said processing result.

4. (Currently Amended) [[An]] The encryption processing method of claim 1 wherein said information processing device and said memory are respectively an arithmetic processing unit and a storage unit to be mounted on an IC card.

5. (Currently Amended) A tamper-resistant fault detection ~~processing~~ method for an IC card including ~~performing a symmetric-key decryption process utilizing~~ an information processing device mounted thereon, comprising the steps of:

(1) performing a symmetric-key decryption process Z = D (C, K) wherein a secret key K is to be applied to an input ciphertext C, and storing the processing result Z on a memory in the IC card;

(2) performing a[[n]] corresponding encryption process W = E (Z, K) for the processing result Z stored on said memory, and storing the result W on the memory;

(3) outputting said processing result Z from said information processing device when said processing result W coincides with said ciphertext C; and

(4) suppressing the output of said processing result Z from said information processing device when said processing result W does not coincide with said ciphertext C.

6. (Currently Amended) [[A]] The decryption processing method of claim 5 wherein said encryption process and said decryption process are executed according to the DES (data encryption standard).

7. (Currently Amended) ~~An encryption~~ The decryption processing method of claim 5 wherein said information processing device is reset as a method of suppressing the output of said processing result.

8. (Currently Amended) ~~An encryption~~ The decryption processing method of claim 5 wherein said information processing device and said memory are respectively an arithmetic processing unit and a storage unit ~~to be mounted on an IC card~~.

9. (Currently Amended) A tamper-resistant fault detection ~~processing~~ method for an IC card including ~~performing an asymmetric-key encryption process utilizing~~ an information processing device mounted thereon, comprising the steps of:

(1) performing an asymmetric-key decryption process Z = D (C, X~~, J~~) wherein a secret key X ~~and a public key information J are~~ is to be applied to an input ciphertext C and storing the result Z in a memory in the IC card;

(2) performing a[[n]] corresponding encryption process W = E (Z, J), wherein a public key J is to be applied to [[for]] the result Z on said memory and storing said result W on the memory;

(3) outputting the processing result Z from said information processing device when said processing result W coincides with said ciphertext C; and

(4) suppressing the output of the processing result Z from said information processing device when said processing result W does not coincide with the ciphertext C.

10. (Currently Amended) ~~An encryption~~ The decryption processing method of claim 9 wherein said encryption process and said decryption process are executed according to RSA cryptosystem.

11. (Currently Amended) ~~An encryption~~ The decryption processing method of claim 9 wherein said information processing device is reset as a method of suppressing the output of said processing result.

12. (Currently Amended) ~~An encryption~~ The decryption processing method of claim 9 wherein said information processing device and said memory apparatus are respectively an arithmetic processing unit and a storage unit to be mounted on an IC card.